Hindawi
Security and Communication Networks
Volume 2022, Article ID 9257443, 11 pages
https://doi.org/10.1155/2022/9257443

Research Article

Post-Quantum Secure Password-Authenticated Key Exchange Based on Ouroboros

Hao Wang,[1,2] **Yu Li**,[1,2] **and Li-Ping Wang**[1,2]

[1]*State Key Laboratory of Information Security, Institute of Information Engineering, CAS, Beijing 100195, China*
[2]*School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China*

Correspondence should be addressed to Li-Ping Wang; wangliping@iie.ac.cn

Received 30 November 2021; Accepted 13 May 2022; Published 14 July 2022

Academic Editor: Youwen Zhu

Password-authenticated key exchange (PAKE) protocols play an important role in cryptography. Most of PAKEs are based on the Diffie–Hellman key exchange protocols or RSA encryption schemes, but their security is threatened by quantum computers. In this study, we propose the first code-based PAKE protocol based on Ouroboros, which is a code-based key exchange protocol. Our scheme enjoys high efficiency and provides mutual explicit authentication, with a security reduction to decoding random quasi-cyclic codes in the random oracle model.

1. Introduction

Authenticated key exchange (AKE) allows two communicating entities to establish a common and high-entropy secret session key over an insecure communication network. In general, users need to store some prepared long-time secret keys with high entropy in devices such as smart cards and ID cards. However, the access to hardware devices makes AKE more inconvenient and complex.

To solve this shortcoming, password-authenticated key exchange (PAKE) was proposed since PAKEs only require human-memorable passwords with low entropy, such as six to eight characters. Nowadays, more and more people tend to use handheld devices, and so PAKEs have a wide range of practical applications. Nevertheless, it is difficult to design a secure key exchange protocol based on passwords, because the low entropy of a password makes it vulnerable to dictionary attacks if an adversary can get some password-dependent data. Generally speaking, there are two types of dictionary attacks. The first one is an online dictionary attack. In this attack, an adversary actively participates the execution of a protocol. For example, an adversary runs a protocol with a guessed password and observes whether the protocol succeeds. However, this type of attack is easy to avoid by just allowing an adversary to test at most a constant number of passwords per online interaction. What we need to consider is the another dictionary attack, i.e., offline dictionary attack. In this attack, an adversary can observe the execution of a protocol or interacts with the participants of the protocol. Next, the adversary tests the correctness of a guessed password offline. To avoid this attack, session keys and protocol messages must look computationally independent from passwords to the adversary.

The first PAKE protocol was proposed by Bellovin and Merritt in [1], which is called the encrypted key exchange (EKE) protocol, but they did not give a formal security proof in the protocol. Since then, a number of PAKE protocols were proposed [2–7]. However, these protocols still have no formal security proof. Until 2000, the formal security models began with the works of Bellare et al. [8] and Boyko et al. [9]. Canetti et al. introduced the universally composable notion to PAKE security model in 2005 [10].

With the security model, plenty of protocols have been designed and analyzed. On the one hand, most of PAKEs are designed using the Diffie–Hellman (DH) key exchange protocols [9, 11–15], in which the PAK [9] and PPK [15] protocols are two efficient and simple constructions of PAKEs based on the DH key exchange protocol. The PAK protocol is three-pass protocol and provides explicit authentication, and the PPK protocol is two-pass protocol and provides implicit authentication. On the other hand, some